


# OPTENET Security Suite PC

Versión 10.09.71



# COPYRIGHT



# ATRIBUCIÓN DE MARCAS COMERCIALES

OPTENET, EDUNET, COTENET, E-OPTENET, OPTENET.BE, OPTENET.CL, OPTENET.CO.CR, OPTENET.COM.EC, EDUNET.COM.ES, OPTENET.COM.ES, EDUNET.ES, OPTENET.ES, OPTENET.US, OPTENET.FR, OBTENET.COM, OBTENET.NET, OPTENET.COM, OPTENET.NET, CAPITANNET.COM, CAPITANNET.ORG, CAPITANNET.NET, CAPITANET.COM, CAPITANET.ORG, CAPITANET.NET, OPTENET.BIZ, PROTEGELES.COM, PROTEGELES.NET, PROTEGELES.ORG, SURF-MATE.COM, SURF-MATE.NET, SURF-MATE.ORG, PROTEGELOS.COM, PROTEGEALOSNINOS.COM, SIFT-PLATFORM.ORG, OPTENET.COM.GT, OPTENET.COM.HN, OPTENET.COM.MX, OPTENET.COM.PA, OPTENET.COM.PE, PTENET.CO.UK (en trámite), optenet.com.ve, son marcas comerciales registradas o marcas comerciales de OPTENET S.A. y/o sus afiliados en España y/o en otros países. Las demás marcas comerciales registradas o sin registrar aquí mencionadas son propiedad exclusiva de sus respectivos propietarios.

# INFORMACIÓN DE LICENCIA

**ACUERDO DE LICENCIA**

AVISO A TODOS LOS USUARIOS: LEA ATENTAMENTE EL ACUERDO JURÍDICO APROPIADO CORRESPONDIENTE A LA LICENCIA QUE HA ADQUIRIDO. EN ÉL SE EXPONEN LOS TÉRMINOS Y CONDICIONES GENERALES QUE RIGEN EL USO DEL SOFTWARE CON LICENCIA.


JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN Y CIENCIA



# ÍNDICE








# 1 INTRODUCCIÓN

## 1.1 OPTENET Security Suite

**OPTENET Security Suite** es una herramienta que le permite optimizar el uso de Internet, al mismo tiempo que le ofrece las mejores garantías de seguridad. Ofrece la protección más eficaz existente en el mercado tanto para los equipos informáticos como para los usuarios de los mismos.

Esto se logra tanto por la gran eficacia de sus componentes particulares como por la óptima combinación de los mismos.

Asimismo, OPTENET Security Suite es una aplicación transparente que no afecta al funcionamiento de las demás aplicaciones existentes, ni al rendimiento de los equipos informáticos, ni a la velocidad de las comunicaciones.

## 1.2 Filtro Web de Contenidos de OPTENET Security Suite

El Filtro de contenidos es un software de fácil instalación que permite evitar el acceso a contenidos no deseados de Internet, como sitios pornográficos, descarga de archivos peligrosos, servidores de mensajería instantánea, P2P, etc.

El Filtro de contenidos es responsable de capturar el tráfico que entra y sale del PC. Además de identificar el tipo de tráfico, solicita al servicio integrado correspondiente que analice, monitorice o rastree el contenido, de modo que pueda garantizar al usuario una navegación segura en función de los parámetros configurados.

Se basa en el análisis semántico de contenidos de sitios web y listas de sitios clasificados en diversas categorías de contenido. Las listas se actualizan cada diez minutos. El análisis semántico verifica, independientemente de si el sitio pertenece o no a la lista, si éste posee algún texto de contenido inapropiado, en cuyo caso se bloqueará para el usuario.






## 1.3 Filtrado de Protocolos

El filtrado de protocolos detecta conexiones e identifica el tipo de protocolo, realizando diferentes acciones en función de la configuración. De esta forma, los usuarios pueden controlar aplicaciones como la mensajería instantánea, los programas P2P, el chat, el correo electrónico y los grupos de noticias.

## 1.4 Idiomas de OPTENET Security Suite

OPTENET Security Suite filtra los principales idiomas utilizados en Internet con una eficacia superior al 98%. Las listas de Security Suite contienen páginas de todos los idiomas. Además, el analizador semántico se entrena periódicamente con páginas de todo el mundo, lo que le permite detectar páginas en todo tipo de idiomas.

Para alcanzar el grado de eficiencia máximo (99%), en determinadas áreas geográficas se establece un conjunto de páginas suficientemente amplio para el entrenamiento del analizador semántico, como por ejemplo en español, inglés, francés, holandés, portugués, alemán e italiano.

## 1.5 Velocidad de Navegación en Internet usando OPTENET Security Suite

La Suite de Seguridad es extremadamente rápido y, por lo tanto, imperceptible desde el punto de vista del usuario. Tanto la consulta de las listas como el proceso de análisis de contenido realizados por el sistema tardan una milésima de segundo. Se trata de una consulta inmediata.

## 1.6 Seguridad del filtro Web de contenidos

Si alguien intenta burlar el filtro, el acceso a Internet se bloqueará completamente como medida de protección. Sólo es posible restablecer el acceso utilizando una contraseña.

## 1.7 Servicio de desbloqueo de Páginas bloqueadas por error

Security Suite posee un margen de error de cerca del 0,1%, el más bajo del mercado. Además, dispone de un servicio de desbloqueo. Si una página se bloquea por error, el usuario puede enviar automáticamente un correo electrónico dirigido a nuestro Centro de Atención al Cliente (CAC) exponiendo el motivo del error para su corrección. El usuario volverá a tener acceso a esa página en 15 minutos aproximadamente.

## 1.8 Activación o Desactivación de la Security Suite

Security Suite se activa o desactiva mediante una contraseña para que los administradores puedan navegar sin restricciones. La contraseña se le solicita al usuario en el momento de la instalación. En caso de que no se disponga de la contraseña, o si alguien intenta desactivar Security Suite, el sistema dispone de mecanismos de autoprotección para que sea imposible desactivarlo.

## 1.9 Bloqueo de Programas de intercambio y descarga de archives P2P

Es posible bloquear los programas de intercambio y la descarga de archivos P2P dentro de la configuración de protocolo del Filtro de contenidos. La categoría de servidores P2P también puede bloquearse, ofreciendo así un mayor nivel de eficacia.

## 1.10 Bloqueo de Programas de mensajería Instantánea

Es posible bloquear los programas de mensajería instantánea dentro de la configuración de protocolo del Filtro de contenidos. La categoría de servidores de mensajería instantánea también puede bloquearse para ofrecer un mayor nivel de eficacia.

## 1.11Actualizaciones

El sistema se actualiza automáticamente a través de Internet. Este proceso no requiere administración.








# 2 REQUISITOS TÉCNICOS

## 2.1 Conocimientos Técnicos

El programa ha sido diseñado para que pueda ser instalado sin problemas por usuarios con conocimientos básicos de informática.

## 2.2 Compatibilidad de Sistemas

La OSSPC está disponible para los siguientes Sistemas Operativos:

- Guadalinex 7
- Guadalinex 6
- Ubuntu 8.04 LTS (Hardy Heron)
- Ubuntu 9.04 (Jaunty Jackalope)
- Ubuntu 9.10 (Karmic Koala)
- Ubuntu 10.04 (Lucid Lynx)

Se aconseja instalarlo en sistemas con mínimo un 1GB de RAM.

Puede ser utilizado con cualquier navegador web.

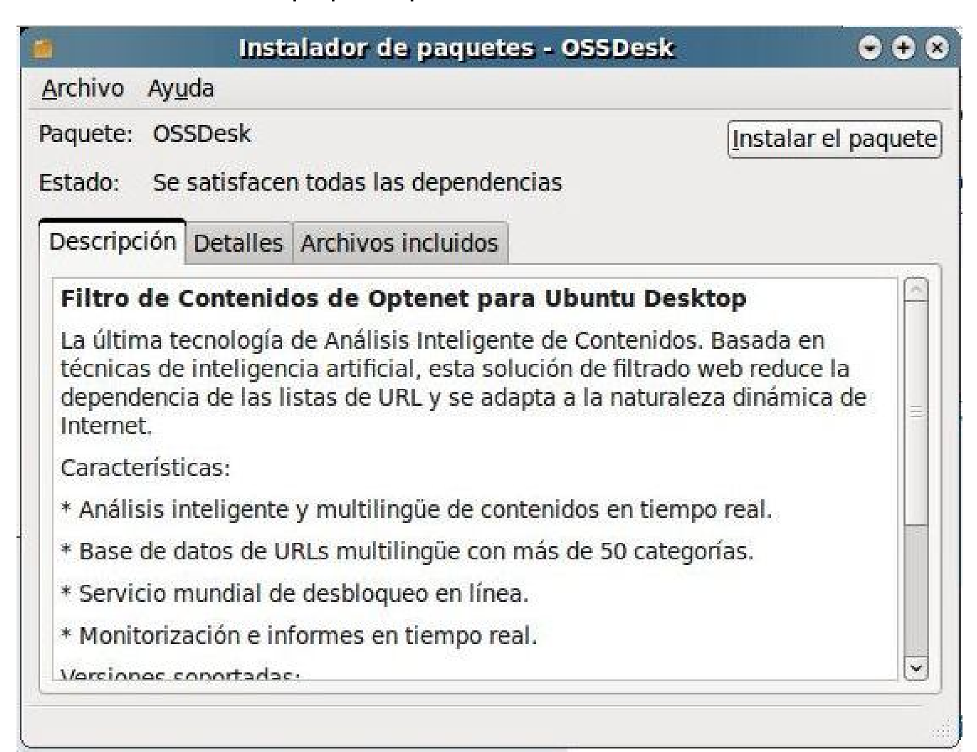


# 3 INSTALACIÓN

Tanto si descarga la aplicación desde una página web, como si lo va a instalar desde un CD, le recomendamos que guarde el programa en el disco duro del PC y siga estos pasos:

1) Haga doble click en el archivo ejecutable de Optenet (tendrá un nombre similar a *OSSDesk-10.09.71.ubu8.ja.deb*)

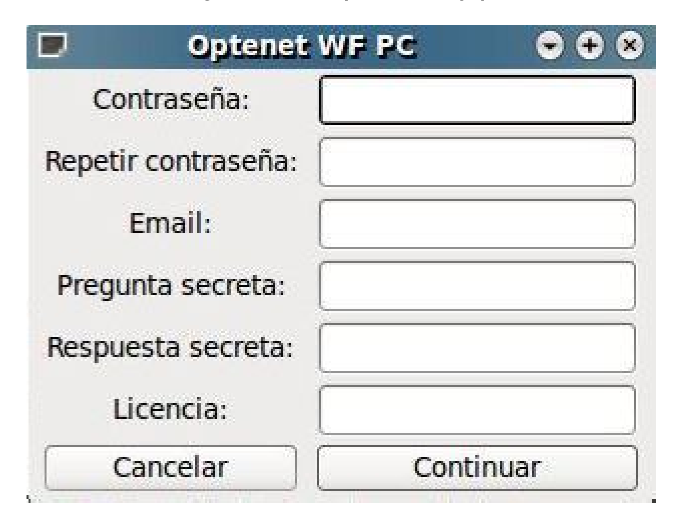
2) Pulse el botón "instalar el paquete" para comenzar la instalación:




3) A continuación, introduzca su contraseña de usuario de su ordenador y pulse el botón Aceptar:




4) A continuación le pedirá que introduzca la contraseña que va a utilizar como administrador del filtro, que complete las casillas relativas a la Pregunta y Respuesta que deberá dar en caso de que olvide su contraseña o la introduzca tres veces erróneamente y que introduzca el código de licencia que le ha sido entregado con el producto y pulse el botón Continuar:




5) El programa de instalación instalará todos los elementos de OSSPC:




6) Por último, el instalador le informará de la finalización del proceso deinstalación. Pulse sobre Cerrar. Ya puede empezar a configurar y utilizarsu OSSPC.

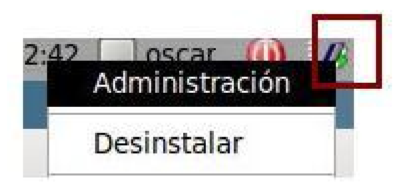







# 4 CONFIGURACIÓN

Vd. podrá acceder a la Consola de OPTENET Security Suite haciendo click con el botón derecho del ratón sobre el icono situado en la barra de estado de Guadalinex y, seleccionando la opción del menú desplegable *[Administración]*.




La contraseña de administración será requerida para evitar el acceso no autorizado (la contraseña indicada en el momento de la instalación del Software).




Una vez haya introducido correctamente la contraseña, se mostrará la consola de Administración:

Optenet Security Suite

Contacto

JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN Y CIENCIA

OPTENET SECURITY SUITE PC

GENERAL | WEB / WAP | CORTAFUEGOS | INFORMES

» General » Estado de las Aplicaciones

ESTADO DE LAS APLICACIONES
CAMBIAR SU CONTRASEÑA
ACTUALIZACIÓN DE SOFTWARE

Control Parental — Servicio ENC.

Firewall — Servicio ENC.

La suite de Seguridad de OPTENET está clasificada en las siguientes secciones:

- General
- Web/Wap
- Cortafuegos
- Informes

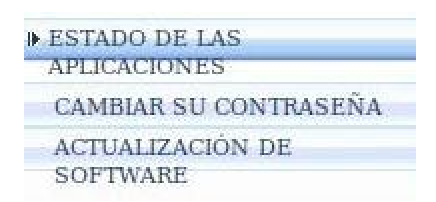


# 5 GENERAL

Esta sección proporciona información sobre la herramienta y los servicios incluidos, permitiendo efectuar tareas de configuración de carácter general como:

- Habilitar/deshabilitar los Servicios.
- Cambio de la Contraseña de Administración.
- Configuración de la actualización del Software.

Al hacer click sobre la pestaña [*General*], el siguiente menú será mostrado a la izquierda de la consola:

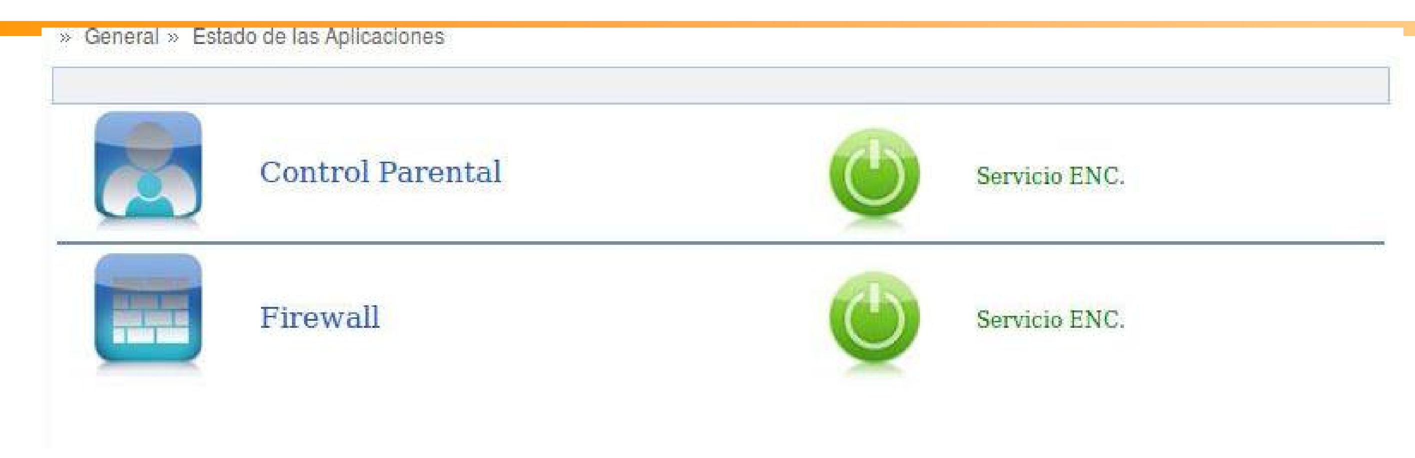



## 5.1 Estado del Servicio

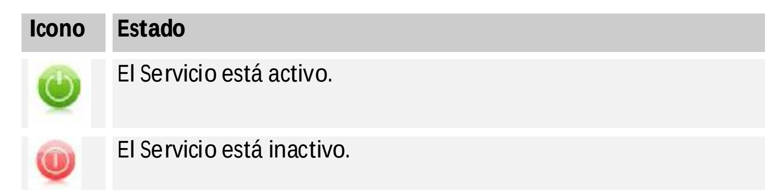
La Suite de Seguridad de OPTENET para la Junta de Andalucia incluye los servicios:

- Filtro de Contenidos (control parental),
- Firewall de protocolos

En esta sección, podrá activarlo o desactivarlo presionando el botón que se encuentra al lado del nombre del servicio.




Un icono diferenciado indicará si el Servicio está activo o no actualmente. En caso de que un Servicio no esté activo, no serán aplicadas las restricciones establecidas.



| Icono | Estado |
|---|---|
| (verde) | El Servicio está activo. |
| (rojo) | El Servicio está inactivo. |

## 5.2 Cambiar su Contraseña

Esta sección permitirá:

- El cambio de la Contraseña de Administración.
- El cambio de la Pregunta/Respuesta de control (a ser utilizadas en caso de que olvide la Contraseña de Administración).



General >> Cambiar contraseña >> Ver detalles

**>> Ver detalles**

-Si olvida su contraseña, aparecerá esta pregunta y, si proporciona la respuesta correcta, se le enviará la contraseña a la dirección de correo electrónico que especifique aquí.
Por ejemplo, podría especificar la pregunta "¿Cuál es el nombre de mi gato?", con la respuesta "Félix". La respuesta distingue entre mayúsculas y minúsculas: Félix no es lo mismo que félix, fÉlix etc.
Tenga en cuenta también que esta pregunta se mostrará a cualquier que intente (sin éxito) acceder a las páginas de configuración. Por este motivo, debe elegir una pregunta de la que sólo usted conozca la respuesta.-

Frase o pregunta: código de empleado de mi prim
Respuesta: a-245xj
Correo electrónico: julian.martinez@gmail.com

Aceptar | Volver

## 5.2.1 Cambio de la Contraseña de Administración

Es decir, la contraseña que permite el acceso a la administración de la Suite de Optenet que fue introducida por primera vez durante la instalación del Producto.

Recuerde que esta Contraseña evita el acceso no autorizado de forma que la configuración solo pueda ser efectuada por el administrador.

A fin de cambiar la Contraseña:

- Introduzca su Contraseña actual.
- Introduzca la nueva Contraseña (y confírmela introduciéndola nuevamente).








### 5.2.2 Cambio de la Pregunta/Respuesta de Recuperación de Contraseña y la dirección de Correo

» General » Cambiar su contraseña

**Cambiar su contraseña**

Escriba su contraseña actual:

Escriba su nueva contraseña:

Confirme su nueva contraseña:

Aceptar | Ver detalles | Cancelar

Desde la ventana [*Cambiar su Contraseña*], haga click en el botón [*Ver Detalles*]. Se mostrará una nueva ventana en la que se podrá cambiar:

- La Pregunta / Respuesta de Seguridad. Obsérvese que la respuesta es sensible a mayúsculas / minúsculas.

  y/o

- La dirección de Correo.




Una vez haya guardado estos cambios, en caso de haber olvidado la Contraseña de Administración y haberla olvidado, tan solo será preciso hacer click en el enlace que aparece en la parte inferior de la ventana:




Se mostrará una ventana en la que se solicita la respuesta a la pregunta de Seguridad:




- En caso de respuesta correcta, la contraseña se enviará al correo del administrador




## 5.3 Nuevas Versiones (Actualización de Software)

OPTENET Security Suite puede actualizarse automáticamente de forma que Vd. no tendrá que preocuparse por nuevas versiones.

Seleccione la actualización de software desde el menú correspondiente.

» General » Actualización de software

**Actualización de software**



☑ Habilitado



# 6 WEB/WAP

Esta sección permitirá la configuración del comportamiento de la herramienta en lo relativo al filtrado web (restringir el acceso a sitios web de contenido inapropiado, la descarga de ciertos tipos de ficheros etc.).

Al hacer click sobre la pestaña [Filtro de Contenidos], el siguiente menú será mostrado a la izquierda:




## 6.1 Opciones

Desde el menú [*Opciones*] de Web/Wap, es sencillo indicar qué tipo de contenidos estarán accesibles para los usuarios.

La ventana estará dividida en secciones diferenciadas:

- SafeSearch (Búsqueda Segura).
- Categorías a bloquear
- Tipos de Archivos a filtrar

### 6.1.1 SafeSearch

Seleccione si desea que SafeSearch de Google (y de otros buscadores) ha de habilitarse por defecto (independientemente de lo configurado por el usuario en el propio buscador).

» Configuración del filtro

☐ Búsqueda segura






### 6.1.2 Seleccionando las Categorías Web a bloquear

Seleccione las Categorías a bloquear: Las páginas web que hayan sido clasificadas bajo esas categorías serán bloqueadas.

Por defecto, algunas categorías ya habrán sido marcadas:

Categorías a bloquear

| | | | | |
|---|---|---|---|---|
| ☐ alcohol y tabaco | ☐ almacenamiento en línea | ☑ anonimizadores | ☑ anorexia y bulimia | Seleccionar todo |
| ☐ azar | ☐ banners | ☑ bombas | ☐ chat | Limpiar todo |
| ☐ correoweb | ☑ drogas | ☐ encuentros | ☐ foros | |
| ☐ fotos y videos | ☐ hackers | ☐ juegos | ☐ juegos adultos | |
| ☐ mensajería instantánea | ☑ modelos | ☐ música | ☑ pornografía | |
| ☐ páginas personales | ☑ racismo | ☐ radio y tv en línea | ☐ redes sociales | |
| ☐ rosa | ☐ salud | ☑ sectas | ☐ servidores p2p | |
| ☑ sexualidad | ☐ spyware | ☑ violencia | | |

**Alcohol y tabaco**: sitios web que venden y/o promueven el uso de tabaco y alcohol para consumo humano, así como productos directamente relacionados con su ingesta.

**Juegos de azar**: sitios web que permiten el acceso a casinos y salas de bingo por Internet, así como a concursos basados en SMS. Esta categoría incluye sitios web en los que pueden realizarse todo tipo de apuestas y también los que ofrecen instrucciones para jugar o que promueven activamente este tipo de actividades

**Compras**: sitios web a través de las cuales pueden realizarse compras de diversos productos y servicios. Sitios que permiten la compraventa entre particulares o entre empresas y particulares. Se incluyen las ofertas de vehículos e inmobiliaria, incluso si las transacciones no se realizan directamente. No incluye apuestas, viajes ni instituciones financieras.

**Foros**: sitios web de carácter temático donde se puede participar aportando opiniones personales.

**Juegos para adultos**: sitios con juegos de naturaleza violenta, erótica o pornográfica; también juegos con temáticas racistas, sectarias y discriminatorias. Incluye los juegos abiertos multijugador en los que la acción puede derivar hacia los contenidos mencionados.

**Sitios web personales**: sitios web personales creados por usuarios de todo el mundo para presentarse a sí mismos o presentar determinados temas de su interés.

**Redes sociales**: sitios web específicamente diseñados al establecimiento de comunidades en línea, en las que los usuarios comparten información entre sí. Estos sitios pueden tener propósitos profesionales o de ocio. No se incluyen los sitios dedicados a relaciones y a contactos entre adultos.

**Sexualidad**: Información y artículos sobre sexo, educación sexual, tendencias sexuales, etc., que no contienen pornografía.

**Almacenamiento en línea**: sitios web que ofrecen a los usuarios la posibilidad de almacenar en línea un gran número de archivos, ya sea con el objeto de compartirlos como para uso personal. No incluye P2P.

**Banners**: banners de publicidad insertados en páginas web. Incluyen los sitios que los sirven.

**Correo web**: sitios web a los que pueden enviarse y en los que pueden recibirse mensajes de correo electrónico.

**Fotos y vídeos**: sitios web que alojan y permiten la publicación y visionado de imágenes y vídeos. Esta categoría no incluye la fotografía artística y profesional.

**Servidores de mensajería instantánea:** sitios web desde los que pueden descargarse programas. Incluye sitios web que permiten el envío de SMS desde Internet.

**Pornografía**: sitios web con contenidos pornográficos u obscenos. Esta categoría incluye el acceso a los chats en los que puede encontrarse este tipo de materiales.

**Rosa**: sitios web con contenidos relativos a famosos; además, contenidos como moda, decoración, etc.

**Software espía**: Sitios web que contienen software espía (spyware). El software espía es un programa que recoge información de un PC y la transmite a fuentes externas a través de Internet. Todo esto tiene lugar sin el conocimiento o la autorización del propietario del ordenador.

**Anonimizadores**: sitios web que permiten a los usuarios navegar por Internet y acceder a contenidos sin quedar registrados por terceros.

**Bombas (y armas)**: Páginas web que explican cómo preparar, construir, distribuir y utilizar explosivos y artefactos explosivos. También sitios de información, promoción o venta de armas de fuego y armas blancas sea para uso militar, deportivo o caza. No se incluyen en esta categoría los cuchillos de bolsillo ni de cocina. Esta categoría sí incluye personas u organizaciones que promueven el terrorismo. También incluye sitios relacionados con armas, municiones y artículos para artes marciales y defensa personal (por ejemplo, pulverizadores, puños americanos), así como artículos de coleccionismo afines.

**Drogas y medicamentos**: sitios web que fomentan el consumo de drogas o facilitan contactos / lugares donde poder adquirirlas. Incluye sitios que venden directamente medicamentos bajo receta sin supervisión de un médico. No se incluyen sitios informativos / preventivos sobre drogas.

**Hackers**: sitios web en los que es posible encontrar software ilegal, así como información para acceder ilícitamente a sistemas informáticos, dispositivos de hardware u ordenadores personales (intrusión).

**Modelos**: sitios web que contienen fotografías de modelos; aquellos sitios en los que tipo de fotos retratan modelos total o parcialmente desnudos están incluidos en la categoría de pornografía.

**Racismo**: sitios web de contenido abiertamente xenófobo o que incitan a comportamientos racistas por motivos de cultura, raza, orientación sexual, religión, ideología, etc.

**Sectas**: sitios web de sectas peligrosas, como los así llamados adoradores de Satán.

**Violencia**: sitios web con contenidos abiertamente violentos, que incitan a la violencia o hacen apología de la misma.

**Anorexia y bulimia**: sitios web dedicados a promover e instigar trastornos de la alimentación.

**Chat**: sitios web a través de los cuales es posible comunicarse con otros usuarios en tiempo real.

**Encuentros, Relaciones**: Sitios web a través de los cuales es posible conocer a otras personas: búsqueda de pareja, relaciones, etc.

**Juegos**: sitios web en los que se puede jugar en línea o desde los cuales pueden descargarse videojuegos.

**Música**: sitios web desde los cuales es posible adquirir o descargar música, o bien encontrar información relativa a cantantes y grupos musicales en general.

**Radio y TV por Internet**: sitios web de emisoras de radio y canales de televisión. Incluyen aquellos que efectúan retransmisiones en línea.

**Servidores P2P**: sitios web que incluyen aplicaciones y programas P2P.

### 6.1.3 Tipos de Fichero a ser bloqueados

A parte de filtrar categorías de páginas web, OPTENET permite el establecimiento de restricciones sobre los ficheros que pueden ser descargados. Especifique aquellas extensiones de ficheros a bloquear.




Existirán dos listas:

- Ficheros cuya descarga está permitida.
- Ficheros a bloquear.

Por defecto, todo tipo de fichero estará permitido.

En ambas listas, los ficheros estarán organizados en "familias":

- Archivos comprimidos
- Imágenes
- Música
- Programas
- Video

Otras estensiones. Obsérvese que bajo las listas existe una sección que permite la introducción de extensiones de ficheros adicionales a ser bloqueadas, haciendo posible el filtrado de todo tipo de ficheros

El filtro de Optenet efectúa "Análisis del Contenido" a fin de detectar tipos de fichero aun habiendo sido renombrados con una extensión diferente. Por ejemplo, si se solicita el bloqueo de ficheros mp3 y se renombra el fichero queen.mp3 por queen.gif, el filtro detectaría el tipo real y bloquearía el fichero.

## 6.2 Tabla de tiempos




Esta sección permite el establecimiento de restricciones adicionales en el acceso a internet:

- Si los horarios no han sido activados, la navegación será permitida siempre (a cualquier hora, aplicando obviamente las restricciones de acceso a categorías prohibidas y la descarga de ficheros no permitidos).
- Si se activa el uso de horarios, Vd. podrá establecer límites de tiempo sobre el uso de Internet:
  - » Podrá definir hasta tres franjas horarias por día de la Semana.

    Nota: Si no se establece ninguna franja horaria para un día de la semana, la navegación estará permitida durante todo el día (o hasta que se alcance el máximo número de horas de uso permitidas por día).
  - » Máximo número de horas de navegación por día.

» Máximum número de horas de navegación acumulada en la Semana.

Estas restricciones de uso (Max. Número de horas/día, Max. Número de horas semanales) funcionarán independientemente de la hora del PC.

Podrá activar o desactivar el uso de horarios seleccionando las opciones "**Activado**" o "**Desactivado**".

## 6.3 Listas de URLs Personales (Listas Blancas y Negras)

Será posible la creación de una Lista Blanca de URLs de confianza y de una Lista Negra de URLs a bloquear sin importar la categoría a la que pertenezcan:




- Vd. podrá personalizar el filtro de forma que ciertas páginas sean accesibles aún perteneciendo a categorías prohibidas. Éstas serán las incluidas en la lista de *Páginas Web Permitidas*.

De forma análoga, Vd. podrá evitar que los usuarios accedan a ciertas páginas, sin importar que pertenezcan a categorías permitidas

- Si desea permitir o bloquear una dirección exacta, marque la casilla de verificación existente a tal efecto.

- De no ser así, se bloqueará el dominio completo.

» Ejemplo. Si introduce www.yahoo.com y no marca la casilla "*Solo la dirección exacta*", los siguientes subdominios también serían bloqueados o permitidos según proceda:

- www.yahoo.com/mail
- www.yahoo.com/shooping etc






## 6.4 Contribución – Añadir Sitios web al Filtro

Contribuya con direcciones de Internet que no han sido detectadas por el filtro (URLs no incluidas en las listas de Optenet ni detectadas por el análisis de contenidos) y que Vd. considere que debieran ser incluidas en alguna de las categorías web (páginas de pornografía etc.).

El Departamento de Revisión de Optenet verificará la dirección de contribución y la asignará a la categoría correspondiente.

Cuando la página ha sido revisada, es clasificada como parte de una o más Categorías. Adicionalmente, si nos indica su correo, será informado del tipo de acción que ha sido llevada a cabo en relación con su solicitud de revisión.

A diferencia de las *Listas Personales*, la contribución informa a OPTENET sobre páginas que debieran ser filtradas en beneficio de todos los usuarios.




Si conoce alguna página de Internet a la que cree que se debe restringir el acceso, puede hacérnoslo saber escribiendo la dirección de la página en "Dirección de la página web" y pulsando el botón "Enviar".

Si lo desea puede indicarnos su correo electrónico y recibirá una confirmación de Optenet cuando la dirección haya sido analizada.

Correo electrónico (Opcional):

Dirección de la página web:

http://

Observaciones:

Enviar | Limpiar







# 7 CORTAFUEGOS

En esta sección podrá seleccionar los diferentes protocolos de aplicaciones que se necesita filtrar.

Para ello seleccionar el servicio que se quiere bloquear, presionar el botón *Agregar* y luego el botón *Aceptar.*

» Cortafuegos » Opciones

» Servicios a bloquear

No seleccionado

- stream
- mensajería instantánea
- p2p
- otros
- servicios de red
- transferencia de archivos
- anonimizadores
- voip
- web

Seleccionado

Agregar ▸▸

◂◂ Eliminar

Seleccionar todo

Aceptar

Cancelar





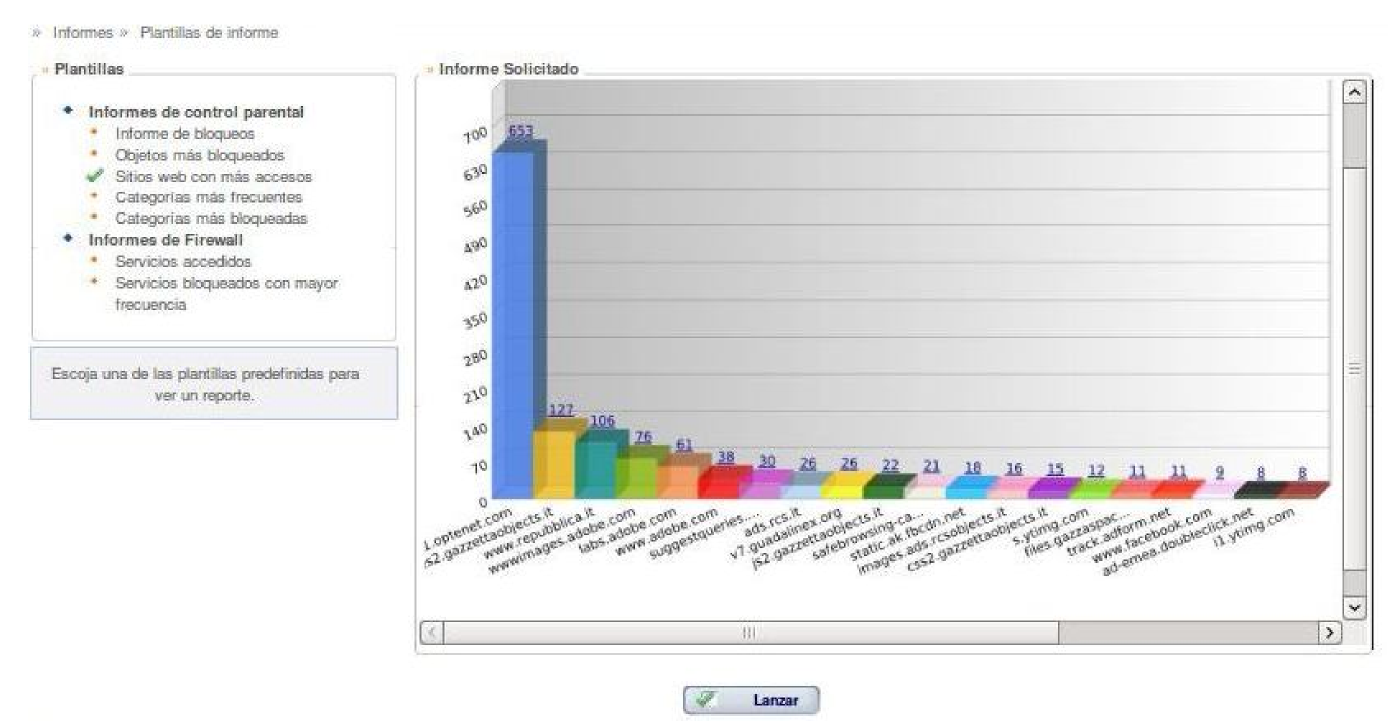




# 8 INFORMES

Vd. podrá consultar qué páginas han intentado ser visitadas por los diferentes usuarios y si el acceso ha sido permitido o bloqueado. Los informes solo mostrarán información de la navegación en aquellos periodos en los que el filtro haya permanecido activo.

Para ello seleccionar en la barra lateral el informe que se quiere generar y presionar el botón *Lanzar.*










# 9 INFORMACIÓN DE CONTACTO




Haga Click sobre el botón [*Contacto*]. Se mostrará una nueva ventana donde se informará de las cuentas de correo a la que puede dirigir:

- Peticiones relacionadas con Atención al Cliente.
- Peticiones relacionadas con Soporte técnico.

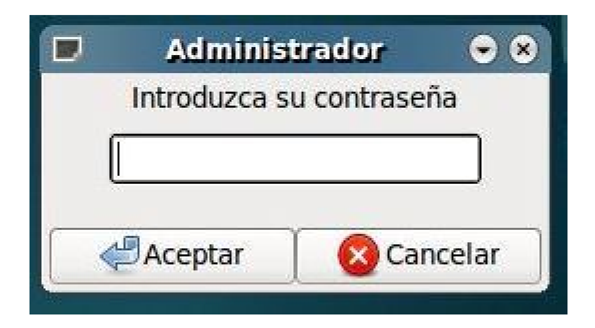


# 10 DESINSTALACIÓN

Para desinstalar la Suite de Seguridad de OPTENET, basta con utilizar el menú accesible con el botón derecho desde el icono del programa en la barra de aplicaciones




Se le pedirá introducir la contraseña de administración de la solución (que se introdujo cuando se realizó la instalación):




IMPORTANTE: No intente desinstalar el programa eliminando los directorios y archivos de la Security Suite, ya que esto podría dañar la instalación de forma irreparable y perder totalmente el acceso a internet. Utilice siempre el acceso directo de su equipo para desinstalar el software.

Si se ejecuta la instalación de OPTENET Security Suite sobre un PC en el que el software ya estuviera instalado, se iniciará el proceso de desinstalación de la versión existente (una vez se haya introducido la contraseña de administración indicada para dicha instalación).